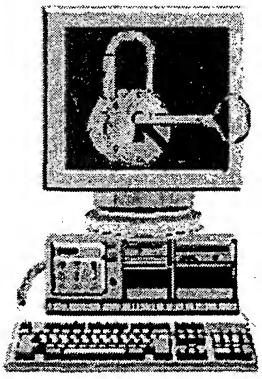
National Digital Mammography Archive

Overview
Networking
Archive
Security
CAD
Education
Partners

Security

Information Security Issues

The NDMA testbed must ensure the privacy and confidentiality of the patients. We will develop and implement multiple levels of system security including access control, encryption, policy definition at enforcement, and the use of virtual private networks. This approach is based on a virtual file room (VFR) concept that allows all active institutional and governmental policies to be accommodated. The security built into this system could provide the foundation for medical information security standards.



Information Security Issues

- Protection of the infrastructure (preventing unauthorized acce to the network or to the network assets
- Access controls and authentication measures to protect acce to the data
- Data integrity and patient confidentiality (stripping identifying factors off the data itself, but ensuring original data is protect and not compromised by changes, compression, etc)

Implications for Shared Applications

- End to end encryption (affects speed, requires decryption, ke management)
- Security within the enterprise (within your control)
- Security external to the enterprise (in someone else's control

trust)
- Security in the archive (privacy, confidentiality, data integrity, authorization)
- Impacts on clinical practice and research (ability to share dat consulting, education)
- Impact on resources and productivity

▲ Top of Page

Healthcare Security and Privacy Drivers

Security in medical applications is being driven by many factors, including public demand, Federal and State legislation, and Federal Regulations. Key among thes the Healthcare Insurance Portability and Accountability Act (HIPAA) of 1996. A Fi Rule on Privacy was released in December, 2000. The Healthcare industry must l compliant with these regulations in two years, The NDMA will work toward the go full HIPAA compliance within the context of the testbed. A summary of HIPAA requirements is presented graphically here.

HIPAA Information Security Requirements

All organizations that handle patient-identifiable healthcare informa are required by the Health Insurance Portability and Accountability of 1996 (HIPAA) to implement policies and technical measures for information protection including:

- Policies and procedures for confidentiality
- Information security infrastructure and training
- Identification and authentication of users
- Access controls based on identity, roles and/or content
- Auditing of user actions
- Communications security
- Information availability and integrity

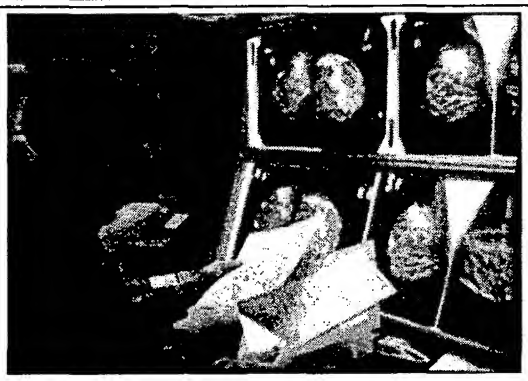
HIPAA Requirements Summary

Administrative Procedures	Policies and practices to implement secur measures
Physical Safeguards	Physical protection of computer and netw assets, facilities, access controls

Technical Security Services	• Access control enforcement • Authentication and identification • Authorization • Auditing and non-repudiation
Technical Security Mechanisms	• Encryption • Data integrity controls • End entity authentication
Additional Safeguards	• Electronic (digital) signatures • Policy negotiation and enforcement

▲ Top of Page

Definitions



- **Privacy** is the ability to control what, when, and with whom y personal information is shared. It is the right of an individual t left alone.
- **Confidentiality** is the act of limiting disclosure of personal information which has been entrusted to another with the confidence that unauthorized disclosure will not occur.

▲ Top of Page

Integrated Multi-level Security Approach

Security Architecture

The NDMA security architecture will ensure patient privacy, meet HIPAA requirements, and conform to federal and medical standarc the use of multiple layers of security services that are robust and mutually supportive. These services include:

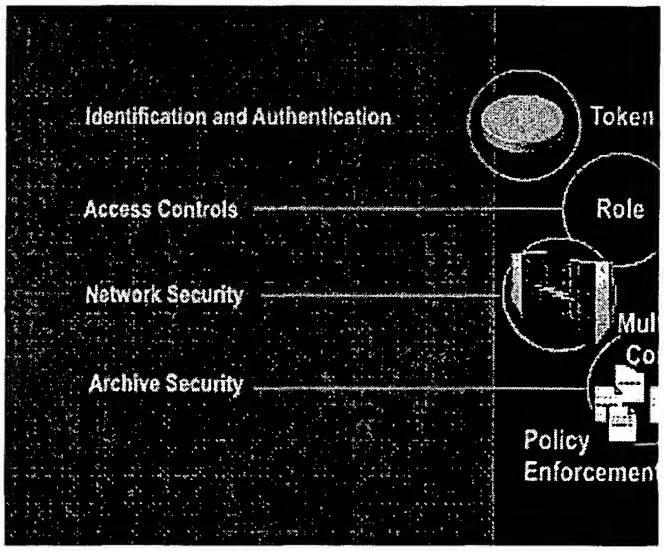
- Physical Security
- Hardware Security
- Software Security
- Communications Security

Multi-Level Security

Goals:

- Protect the infrastructure
- Protect access to data (need to know)
- Ensure data integrity
- Protect the patient's privacy

Implementation:



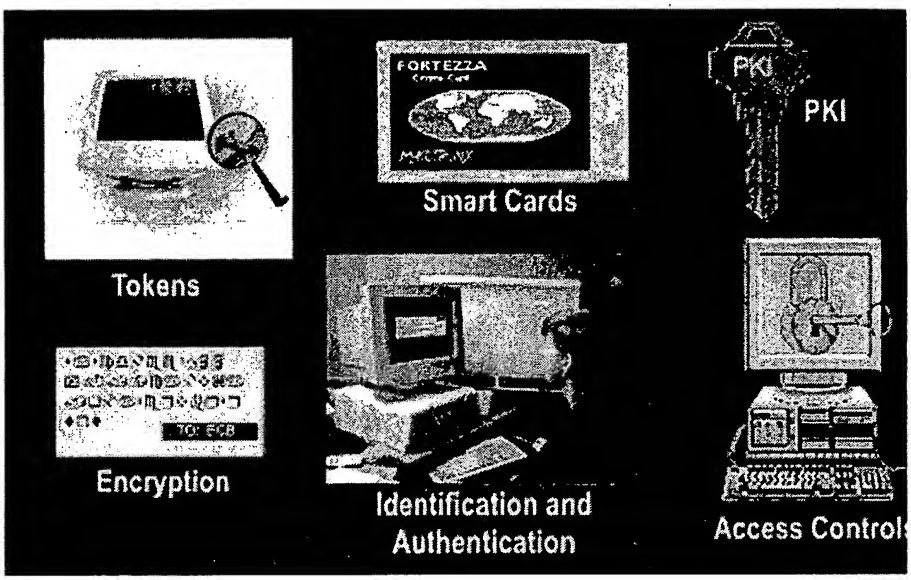
▲ Top of Page

Technologies and Implementation

- Virtual Private Network/ encryption
- Certificates and Smart card authentication
- Login/Password
- Role-Based Access Controls (clinician, researcher, administrator, others tc determined)
- Other authorizations as required (credentials, trusted devices)
- Patient Consent
- Policy Definition and Enforcement at local and archive levels
- Status monitoring

- Removal of patient identifiers when needed

Sample Technologies



Summary

- Information Security must be factored into medical applicatio and emerging technologies
- Federal rules and regulations and public demand are key dri
- Privacy and confidentiality will become bigger factors with electronic data transmission
- Many technologies are available; no single technology offers fully integrated solution
- Medical community needs to be INVOLVED in identifying problems and testing potential solutions

▲ Top of Page

Page updated: March 19, 2001

The National Digital Mammography Archive (NDMA) is funded by the National Library of Medicine under the *Bio-Medical Applications for the Next Generation Internet* program.
For questions or comments contact Mitchell D. Schnall, M.D., Ph.D., University of Pennsylvania.


UNITED STATES
National Library of Medicine